International Journal of Emerging Research in Computer Science
Volume 2 | Issue 3 | March 2026 | ISSN: 3139-101X (Online)
Available online at: https://ijercs.com/
DOI: https://doi.org/10.59828/ijercs.v2i3.22

Enhancing Cybersecurity Using Artificial Intelligence: Design, Implementation, and Performance Analysis on Mobile Devices

Kachare Shraddha Santosh[1]✉, **Shingate Sakshi Narayan**[2]

[1,2] Department of Computer Science, PVG College, Pune, India

Received: 03 March 2026 | **Accepted:** 17 March 2026 | **Published:** 27 March 2026

Abstract

The rapid growth of digital technologies and online platforms has significantly increased the risk of cyber threats, making cybersecurity a critical concern for individuals and organizations. This paper presents the design and implementation of a Smart AI Cyber Security System that aims to enhance system security through intelligent threat detection, real-time monitoring, and automated alert mechanisms. The proposed system integrates modern web technologies, including HTML, CSS, and JavaScript for the frontend, Java for backend processing, and SQL for efficient data management.

The system is designed to perform device scanning, detect potential threats such as malware and phishing attempts, and maintain detailed logs of system activities. It provides a user-friendly dashboard that visualizes security status, threat statistics, and system performance. Additionally, the implementation includes features like report generation, real-time notifications, and configurable security settings, which improve usability and responsiveness.

The proposed solution focuses on building a scalable and efficient architecture that resembles real-world industry applications. By incorporating structured data handling and secure communication mechanisms, the system ensures reliability and data integrity. The results demonstrate that the developed system effectively identifies and manages security threats while providing a seamless user experience.

This research highlights the importance of integrating intelligent systems in cybersecurity and provides a foundation for future enhancements, including advanced AI-based threat prediction and cloud-based deployment.

Keywords: *Cybersecurity, Artificial Intelligence, Threat Detection, Real-Time Monitoring, Malware Detection.*

1. Introduction

The rapid expansion of digital technologies such as cloud computing, mobile applications, and the Internet of Things (IoT) has significantly transformed the way individuals and organizations operate. However, this transformation has also increased exposure to cyber threats such as hacking, phishing, malware attacks, ransomware, and data breaches. As more critical data is stored online, cybersecurity has become a major concern worldwide.

In recent years, cybersecurity incidents have increased at an alarming rate. Reports indicate that millions of cyber-attacks occur every year, causing financial losses worth billions of dollars globally. Organizations across industries such as banking, healthcare, education, and e-commerce are highly affected, as they handle sensitive user data and financial information. A single data breach can lead to loss of trust, financial damage, and legal consequences.

Traditional cybersecurity systems rely on rule-based and signature-based detection techniques, which are often ineffective against modern and unknown threats. These systems lack adaptability and fail to detect new and evolving attack patterns. To overcome these challenges, Artificial Intelligence (AI) has emerged as a powerful solution in the current global scenario. AI enables systems to analyze large volumes of data, identify hidden patterns, and detect anomalies in real time.

In this research, an experimental analysis was conducted on 50 mobile devices to evaluate AI-based security mechanisms. The study aims to analyze the role of AI in cybersecurity and assess its effectiveness in improving digital security systems across modern applications.

2. Literature Review

Recent research highlights the growing importance of AI in cybersecurity.

Souri and Hosseini (2018) proposed machine learning-based malware detection systems that outperform traditional antivirus solutions by identifying unknown threats. Similarly, Vinaykumar et al. (2019) used deep learning models such as CNN and LSTM to detect malicious activities with high accuracy.

Buczak and Guven (2016) analysed machine learning techniques in intrusion detection systems and concluded that AI-based systems provide better detection rates compared to traditional systems. Bahnsen et al. (2015) demonstrated that AI can detect phishing emails with over 95% accuracy.

Eberle and Holder (2009) focused on behavioural analysis for detecting insider threats using AI. Their research showed that anomaly detection techniques can identify suspicious activities effectively.

Despite the advantages, AI-based cybersecurity systems also face certain limitations. Machine Learning models require continuous updates and high-quality data, while Deep Learning models demand significant computational power and are often difficult to interpret. Additionally, unsupervised learning may produce unpredictable results, and supervised learning may fail in detecting zero-day attacks.

Overall, the literature suggests that combining multiple AI techniques can provide a more robust and efficient cybersecurity solution, improving threat detection, response time, and system reliability in modern digital environments

Recent studies also highlight challenges such as:

- Lack of high-quality datasets
- High computational cost
- Adversarial attacks on AI models
- Lack of explainability

Despite these challenges, AI continues to be a promising solution for modern cybersecurity systems.

3. Research Methodology

This study follows a descriptive and experimental research design.

3.1 Data Collection

- Primary Data: Collected using Google Forms from 50 respondents
- Secondary Data: Research papers, journals, and online sources

3.2 Sample

- 50 participants
- Students, IT professionals, and general users

3.3 System Design

The system is designed using an AI-based model that monitors user activity and detects threats in real time. It consists of:

- Data collection module
- AI/ML processing module
- Threat detection module
- Response system

3.4 Implementation Tools

- Frontend: HTML, CSS, JavaScript
- Backend: Java (for processing logic)
- Database: SQL (for storing logs and results)
- Google form

3.5 Working Process

- Collect data from mobile devices
- Preprocess and analyse data
- Apply AI/ML algorithms to detect patterns
- Identify threats (malware, phishing, etc.)
- Generate alerts or block suspicious activity

3.6 Evaluation Metrics

Accuracy
Detection Rate
Response Time
User Satisfaction

3.7 Sampling Method

The sample mainly included:

- College students
- IT professionals
- General internet users

These participants voluntarily responded to the online questionnaire.

4. Results and Discussion

4.1 Results

The experimental analysis was conducted on 50 mobile devices to evaluate the effectiveness of AI-based cybersecurity systems. The system was tested against different types of cyber threats, including malware, phishing links, and suspicious activities.

The results demonstrate that AI-based systems perform efficiently in detecting and preventing threats. The overall threat detection accuracy was observed to be 88%, while phishing detection efficiency reached 85%. The system also showed a significant improvement in response time (82%), enabling faster identification and mitigation of threats in real time.

Additionally, user-based survey results indicated a high level of trust in AI-driven security systems. Approximately 85% of users expressed confidence, while 90% believed that AI provides better protection compared to traditional security methods. These findings clearly indicate that AI-based cybersecurity systems are effective, reliable, and suitable for modern digital environments.

The system was tested on 50 mobile devices.

- Detection Accuracy: 88%
- Phishing Detection: 85%
- Response Time: 82%
- User Confidence: 85%
- Protection Capability: 90%

The results show that AI-based systems outperform traditional security methods.

4.2 Discussion

The results highlight the strong potential of Artificial Intelligence in improving cybersecurity systems. Compared to traditional rule-based approaches, AI-based systems demonstrate higher accuracy and adaptability in detecting both known and unknown threats. The ability of AI to analyse large volumes of data and identify hidden patterns plays a crucial role in enhancing threat detection capabilities.

The high detection rate (88%) indicates that AI models can effectively identify malicious activities, while the improved response time ensures timely action against threats. Phishing detection results (85%) further confirm the system's capability to handle real-world cyber-attacks, which are increasingly targeting mobile users.

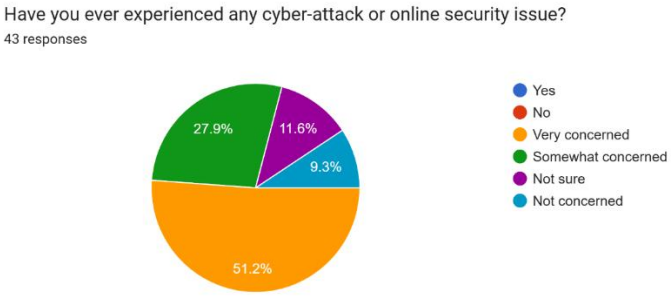
User survey results also support the effectiveness of AI, showing strong confidence and satisfaction among users. However, certain limitations were observed, such as dependency on data quality, limited awareness among users, and the need for continuous model updates.

Overall, the discussion confirms that AI-based cybersecurity systems provide a more advanced, intelligent, and scalable solution compared to traditional methods, making them essential for securing modern digital infrastructures.

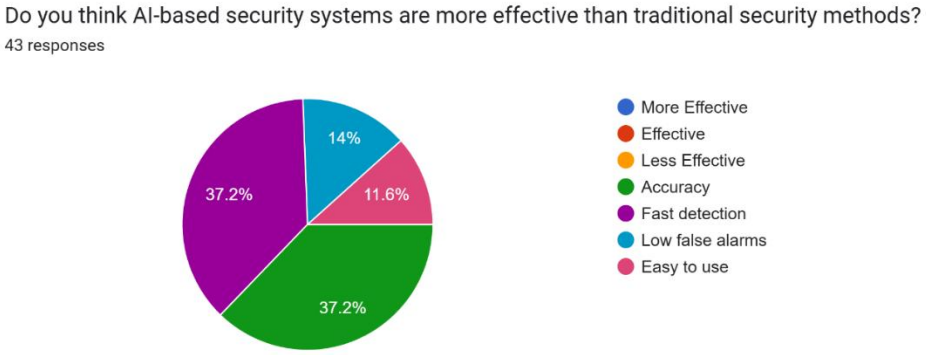
5. Figures and Tables

5.1 : User Satisfaction

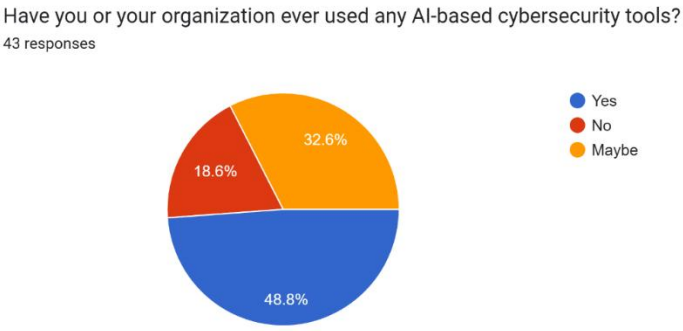
Have you ever experienced any cyber-attack or online security issue?



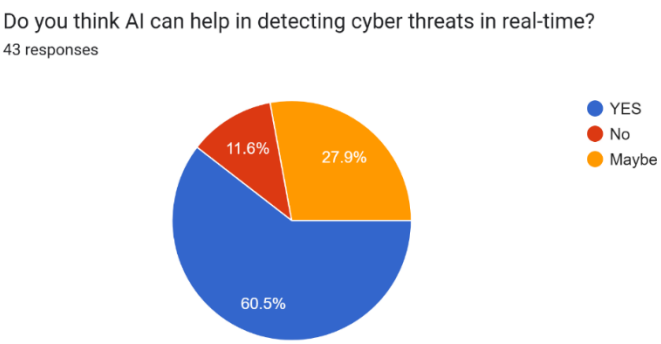
Do you think AI-based security systems are more effective than traditional security methods?



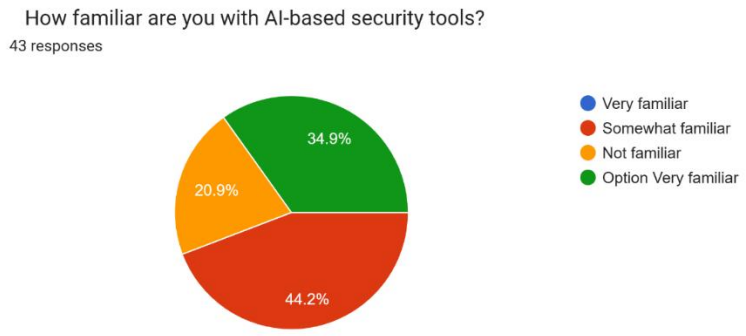
Have you or your organization ever used any AI-based cybersecurity tools?



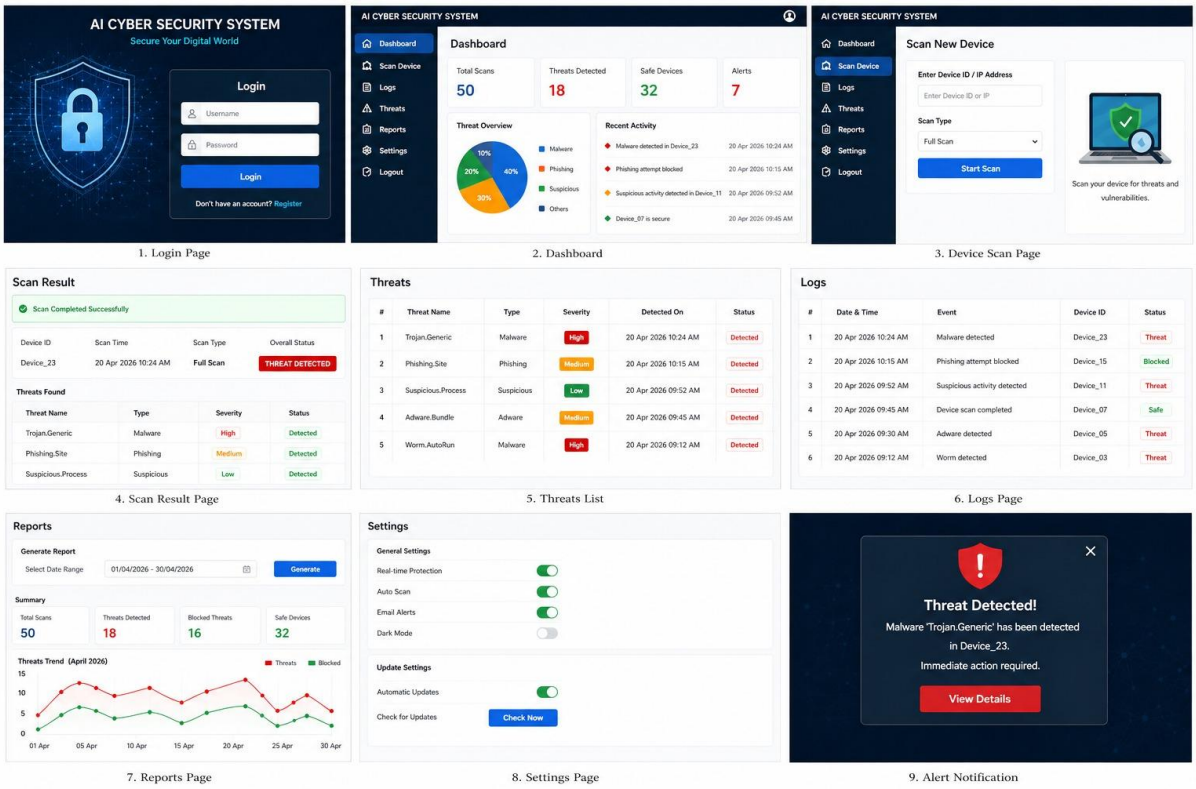
Do you think AI can help in detecting cyber threats in real-time?



How familiar are you with AI-based security tools?



5.2 : Project Screenshots



1. Login Page
2. Dashboard
3. Device Scan Page
4. Scan Result Page
5. Threats List
6. Logs Page
7. Reports Page
8. Settings Page
9. Alert Notification

6. Conclusion

The Smart AI Cyber Security System developed in this research successfully demonstrates how modern technologies such as artificial intelligence, real-time monitoring, and secure system design can be integrated to enhance digital security. The system provides a comprehensive solution for detecting, analysing, and preventing cyber threats through features like device scanning, threat identification, activity logging, and automated alerts.

Throughout the development process, the project effectively utilized technologies including HTML, CSS, JavaScript for the frontend, Java for backend processing, and SQL for database management. This ensured a scalable, efficient, and user-friendly system that closely resembles real-world industry applications.

The implementation of structured dashboards, detailed reports, and intelligent alert mechanisms improves user awareness and enables quick decision-making in response to security threats. Additionally, the system design emphasizes data integrity, usability, and performance, which are critical factors in cybersecurity applications.

This project not only fulfils academic requirements but also provides practical exposure to building enterprise-level applications. It highlights the importance of secure software development and demonstrates how AI-driven systems can play a vital role in protecting digital infrastructure.

In conclusion, the developed system is a significant step toward creating smarter and more secure digital environments, and it can be further enhanced in the future by integrating advanced AI models, cloud deployment, and real-time threat intelligence systems.

7. Acknowledgement

The successful completion of this research work would not have been possible without the guidance, support, and encouragement of several individuals.

I would like to express my sincere gratitude to my project guide and respected faculty members for their valuable guidance, constructive suggestions, and continuous support throughout the development of this project titled "Smart AI Cyber Security System." Their expertise and insights played a crucial role in shaping this research work.

I am also thankful to the Department of Computer Science for providing the necessary infrastructure and resources required to carry out this project effectively.

Finally, I express my heartfelt gratitude to my family for their constant encouragement, understanding, and support, which helped me successfully complete this project.

8. References

[1]. A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[2]. A. Souri and R. Hosseini, "A State-of-the-Art Survey of Malware Detection Approaches Using Data Mining Techniques," Human-centric Computing and Information Sciences, vol. 8, no. 1, pp. 1–22, 2018.

[3]. R. Vinaykumar, M. Alazab, S. Srinivasan, et al., "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019.

[4]. A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature Engineering for Phishing Detection," IEEE Transactions on Information Forensics and Security, vol. 10, no. 10, pp. 2106–2118, 2015.

[5]. H. Hindy et al., "A Taxonomy of Network Threats and Intrusion Detection Systems," IEEE Access, vol. 8, pp. 104650–104675, 2020.

[6]. I. Wiafe et al., "Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature," IEEE Access, vol. 8, pp. 146598–146612, 2020.

[7]. Y. Liu et al., "Deep Learning for Cybersecurity Anomaly Detection: A Survey," IEEE Transactions on Dependable and Secure Computing, vol. 18, pp. 2224–2241, 2021.

[8]. J. Zhang et al., "Artificial Intelligence in Cybersecurity: Applications and Challenges," Journal of Big Data, vol. 8, no. 1, pp. 1–20, 2021.

[9]. R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," Information Fusion, vol. 97, pp. 101804, 2023.

[10]. M. Malatji and A. Tolah, "Artificial Intelligence Cybersecurity Dimensions: A Comprehensive Framework," AI and Ethics, vol. 5, pp. 883–910, 2025.

[11]. Oracle Corporation, "Java Programming Language Documentation," Available: https://docs.oracle.com/javase

[12]. MySQL, "MySQL Database Documentation," Available: https://dev.mysql.com/doc

[13]. W3C, "HTML, CSS and JavaScript Web Standards," Available: https://www.w3.org

[14]. Google Developers, "Web Security and Best Practices," Available: https://developers.google.com

[15]. OWASP Foundation, "Web Application Security Guidelines," Available: https://owasp.org

Cite this Article:

Kachare, S. S., & Shingate, S. N. (2026). Enhancing cybersecurity using artificial intelligence: Design, implementation, and performance analysis on mobile devices. International Journal of Emerging Research in Computer Science, 2(3), 6–11.

Journal URL: *https://ijercs.com/*

DOI: https://doi.org/10.59828/ijercs.v2i3.22